AN APPROACH TO IDENTIFICATION OF MINIMUM TCB REQUIREMENTS FOR VARIOUS THREAT/RISK ENVIRONMENTS

November 14, 1982

James P. Anderson Co.
Box 42
Fort Washington
PA. 19034

An Approach to Identification of Minimum TCB Requirements For Various Threat/Risk Environments *

Introduction

This note attempts to identify the minimum Trusted Computer Base (TCB) required for classified data processing as a function of the clearance(s) of the user population and the highest classification of the data.

We approach the problem by first identifying broad categories of threat/risk and then for each of the categories, identify a minimum TCB that will provide protection suitable to the threat/risk environment.

Remarks on Clearance

For the purposes of this note, we are treating SCI as the highest clearance level in the SCI, Top Secret, Secret, Confidential, Unclassified hierarchy. While strictly speaking, SCI is an "access approval" based on a Top Secret clearance, and is treated as a 'category' in Bell and Lapadula [2], in practice, it does represent a different clearance standard for most holders of such approvals (polygraph verification of PSO data).

The threat/risk diagram shown in Figure 1 is the result of a number of trials at identifying and depicting the relationships involved. The major difficulty that has been encountered arises from the fact that SCI has both hierarchical (discussed above) and disjoint properties. Thus, while a Top Secret clearance is generally adequate for a user to exist in a Top Secret data environment even when he does not have a need-to-know for all of the Top Secret information in the environment, one SCI approval is not adequate for a user to exist in a data environment with other SCI data. These anomalies aside, the general thrust of the threat/risk environment matrix and its interpretation in terms of minimum standards of computer security based on the DODCSC evaluation criteria [1] is believed to be correct. It represents reasonably well what we actually do.

---

* A revision of Appendix I to Comments on DCID 1/16 of July 1, 1982.

Threat / Risk Environment

The diagram, Figure 1, assigns threat/risk categories to the various combinations of classification and clearances.

Maximum Data Classification

Lowest Level User Clearances	U	C	S	TS	SCI
U	1	3	4	4	4
C	1	2	3	4	4
S	1	2	2	4	4
TS	1	2	2	2	3*
SCI	1	2	2	2	2*

* With more than one category of SCI present, raise the threat/risk category number by 1.

Figure 1

Threat/Risk Categories as a Function of Clearance/Classification

As indicated above, SCI is treated as though it is a separate clearance for purposes of evaluating threat and risk. The "meanings" of the category numbers are shown below.

Category	Meaning
1	No threat or risk because there is no classified data present. (included for completeness).
2	No threat or risk:all persons have clearance for the (maximum) classification of data present.
3	Moderate threat/risk, different clearance standards, but adjacent clearances.
4	Maximum threat/risk: different, non-adjacent clearances.

The type of security system required for each threat/risk category is shown in Table 1.

Threat/Risk Category	Type of Use: General (Programming) Use	Type of Use: Transaction Only
1	D(common practice)*	D(common practice)
2	B1(labeled security)	C1(discretionary)
3	B3(security domains)	B2(structured protection)
4	A2(verified implementation)	B3(security domains)

* descriptive terms from [1].

Table 1

Minimum Security Standard for Computer Systems
As a Function of Threat/Risk Category

The threat/risk environments assocated with each category are, for the most part, self-explanatory. Clearly, in the category 1 environment, there is no security threat or risk since there is no classified material involved.

In the case of the category 2 environment, there is no threat or risk since all users are cleared/approved for all material.

The category 3 threat/risk environment, represents a threat due to the uneveness of the clearance standards and a risk of accidental disclosure. However, for appropriate adjacent clearance levels (Confidential-Secret, Top Secret - SCI) where the basic clearance standards are similar (National Agency Check, Proof of Citizenship and some form of Background Investigation, possibly augmented by a polygraph examination in the case of Top Secret - SCI or SCI1 - SCI2) it can be argued that with a suitably secure processor,that the threat and risk can be contained.

The category 4 threat risk environment is the 'multilevel' environment, where the clearance standards are substantially different and/or where uncleared individuals may exist on the system. This environment represents the maximum threat / risk and requires the greatest level of protection that we know how to build. An example of this category is the USAF Data Services

Center in the Pentagon.

Please note that the proposed standards are a MINIMUM and that specific cases can justify higher level systems. Note also that the proposed minimum levels are mandatory. There is NO exception to the requirement, although approving authorities may grant waivers on existing systems until the hardware they are running on is 'upgraded' or replaced.

In general, where the data environment is multi-level (i.e. in System High and Compartmented mode systems), there is a requirement for systems exhibiting higher levels of protection than in Dedicated mode use. This is because even though the threat/risk environment is low to moderate based on the same minimum level clearance (for System High) or whatever justification is used for Compartmented mode, there is a greater risk of mixing data from higher classification files with that of lower classification files and releasing the data as the lower classification. In the case of compartmented mode operation, there is also an increased threat due to the direct access of lower cleared individuals.

Still true

References

[1] Trusted Computer System Evaluation Criteria, May 24, 1982. DoD Computer Security Center.

[2] Bell,D.E., Lapadula,L.J., "Secure Computer Systems", ESD-TR-73-278, Vol I - III, The MITRE Corporation, Bedford, MA, November 1972 - June 1974.